

Export Control Compliance Policy

November 2011

INTRODUCTION

In today's global economy, few companies can grow without exporting their goods and services into foreign markets. Even so, despite the importance of exports in the economy, exporting is a privilege and not a legal right. The U.S. government strictly controls what items may or may not be exported, and under what circumstances. These restrictions are called export controls.

The government regulates export controls for a variety of reasons. Some controls are designed to safeguard domestic supplies and to protect the economy. Others are aimed at protecting the national security and foreign policy interests of the country. Many controls serve more than one purpose.

Export controls can seriously impact Castle's ability to send our products and services abroad legally. Violations of export control laws can result in severe civil and criminal penalties, including fines, prison, seizure of the items in question, and suspension of the right to engage in further export activities.

OVERVIEW OF EXPORT CONTROLS

The government separates its export controls into two basic categories, one for defense items and one for dual-use items (those that can be used for both commercial and military purposes). Defense articles are subject to the International Traffic in Arms Regulations ("ITAR"). Dual-use articles are subject to the Export Administration Regulations ("EAR"). In addition, most items that were initially designed for a military purpose remain subject to the ITAR even if the current use is predominantly commercial.

Although most of the Company's products are not controlled for export, Castle sells products covered by the ITAR and products covered by the EAR. Therefore, it is necessary to evaluate the appropriate controls before selling any Castle product for export to another country. This policy provides an overview of the U.S. export control laws, the administering agencies, and possible penalties.

Department of Commerce Controls

The Bureau of Industry and Security ("BIS") of the U.S. Department of Commerce implements and enforces U.S. export control regulations relating to the export of "dual-use" goods and technologies (having both civil and military applications) as well as exclusively civil items. Items subject to the jurisdiction of BIS are listed on the Commerce Controls List ("CCL") found in the EAR. The CCL covers such things as materials, chemicals, microorganisms, and toxins; materials processing; electronics; computers; telecommunications and information security; lasers and sensors; navigation

and avionics materials; marine-related materials; and propulsion systems, certain space vehicles, and related equipment. The index to the CCL is located [here](http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=95891af86e99b5c9887e271a348aeec7&rgn=div9&view=text&node=15:2.1.3.4.45.0.1.3.87&idno=15).
(<http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=95891af86e99b5c9887e271a348aeec7&rgn=div9&view=text&node=15:2.1.3.4.45.0.1.3.87&idno=15>)

Whether a license is required to export or reexport an item on the CCL is determined by examining the precise classification of the item, the destination of the item, and the end-user. BIS also maintains the Denied Persons List and the Entities List, which identify specific persons and entities to which exports are not permitted without the prior approval of BIS.

Department of State Controls

The Directorate of Defense Trade Controls (“DDTC”) of the U.S. Department of State regulates the export of defense goods, technical data and defense services. DDTC administers the ITAR. Generally, a defense article is an item developed for a military application that does not have a predominant civilian application. The scope of defense articles covered by the ITAR are identified in the United State Munitions List (“USML”). The USML covers such things as guns and armaments, ammunition, launch vehicles and missiles, explosives and other incendiary agents, vessels of war, tanks and military vehicles, aircraft, military training equipment, protective personnel equipment, fire control equipment, auxiliary military equipment (including cameras and cryptographic devices, software, and components), toxicological agents, spacecraft systems, nuclear weapons, and classified articles as well as technical data and services that relate to the enumerated categories. The index to the munitions list can be found [here](#).

Unless an exemption applies, a license must be obtained before any defense article is exported to a foreign country or foreign national. Authorization by DDTC is also required for any agreement under which a U.S. person will furnish assistance to foreign persons in the development, design, production or use of a defense article or under which a U.S. person will license to a foreign party the right to manufacture U.S.-origin defense articles abroad. DDTC maintains a list of “debarred” persons and entities whose exporting privileges have been revoked as a consequence of violations of the ITAR.

Deemed Exports, Exports of Technical Data, and Exports of Defense Services

In addition to regulating the export of actual goods or commodities, U.S. export controls cover the export or release of “technical data” or technology (which includes information, whether printed, inscribed on media, or communicated orally). Under the EAR the release of such information related to dual-use commodities is called a “deemed export”. Under the deemed export rule, the transfer or release of technical data or information subject to U.S. export controls to a “foreign national”, whether it occurs in the United States or abroad, is “deemed” an export from the United States to the home country of the foreign national. When technology is released to a foreign national who is in the United States, that knowledge is considered to have been exported to the foreign nationals’

country or countries of nationality, even if the person never leaves the United States. This rule also applies to U.S. Citizens and permanent residents taking restricted information abroad or accessing the restricted information while abroad.

The ITAR include similar restrictions. Technical data related to an ITAR-controlled product cannot be released to a foreign national or non-U.S. citizen or permanent resident without a license, whether that person is located in the United States or abroad. In addition, as discussed above, the provision of assistance (defense services) to foreign persons in the development, design, production or use of a defense article by a U.S. person may require an ITAR license.

Technology and information relating to any products identified by Castle's Trade Compliance Department as possibly requiring a license should not be shared with any person or removed from the United States without first contacting the Trade Compliance Department.

U.S. Sanctions Programs

Certain restrictions apply to all Castle U.S. and non-U.S. branches' dealings with certain countries, terrorist organizations and parties associated with narcotics trafficking. The U.S. Sanctions Programs can include tariffs, trade barriers, import duties, import or export quotas or other monetary restrictions. The names of parties and individuals subject to these restrictions can be found [here](http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx) (<http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>) or you can send an email to the Trade Compliance Manager to check the name on your behalf. Castle may not have business or financial dealings with parties in or controlled by the government of Cuba, regardless of the circumstances. However, there are "blocking" laws in Canada, Mexico and the European Unions that may in some situations conflict with U.S. sanctions against Cuba. The Legal Department should be contacted immediately in the event of any business proposal opportunity of a non-U.S. Affiliate concerning Cuba.

Anti-Boycott Regulations

The anti-boycott laws were adopted to require U.S. companies to refuse to participate in foreign boycotts that the United States does not sanction. They have the effect of preventing U.S. companies from being used to implement foreign policies of other nations which run counter to U.S. policy.

The Arab League boycott of Israel is the principal foreign economic boycott that Castle employees should be aware of today. The anti-boycott laws, however, apply to all boycotts that are unsanctioned by the United States. No employee of Castle may sell goods, services or technology to customers, governments or nationals of a country participating in the Arab boycott of Israel, or enter into any agreement or contract with any such party, without first contacting the Legal Department to ensure compliance with U.S. Antiboycott laws. Countries that most frequently require language in documents or request information that is unacceptable under U.S. anti-boycott law, based upon the best

information available to the Legal Department, include, but are not limited to: Bahrain, Iraq, Kuwait, Lebanon, Libya, Oman, Qatar, Saudi Arabia, Syria, United Arab Emirates and Yemen.

Requests to participate in the Arab boycott of Israel sometimes emanate from countries, including members of the League of Arab States, not formally identified with the boycott. Very rarely, requests may be received relating to international boycotts (e.g. India/Pakistan; China/Taiwan) other than the Arab boycott of Israel. Responses to any such requests should be cleared through the Legal Department.

EXPORT CONTROL POLICY

It is the policy of Castle to comply fully with all U.S. Government export control laws and regulations. No transactions are to be conducted by or on behalf of Castle contrary to U.S. export regulations. Castle supports U.S. efforts to fight the battle against terrorism and prevent transactions involving entities engaged in prohibited missile, nuclear, chemical and biological warfare activities. Therefore, we have implemented export control procedures that all employees are required to follow. These procedures can be found in the Export Control Management Program, located on our International Trade Compliance Intranet.

1. Any employee of Castle or any U.S. Affiliate engaged in the “export” or “reexport” of goods, software or technology (including consulting services) from the U.S. must determine and document whether an export license issued by the U.S. Department of Commerce – Bureau of Industry and Security, U.S. Department of State – Directorate of Defense Trade Controls, or any other U.S. government agency is required prior to shipment and, if so, ensure that the requisite license has been obtained before export. Castle’s International Trade Compliance Department reviews Castle products to identify those regulated for export and that may require a license. Such products may be identified on Castle’s Intranet system and/or in Castle’s ERP system(s) of record. However the absence of any material within these systems should not be construed as that of not requiring a license. All required shipping documentation must be completed, and copies of all export documentation must be retained for at least 5 years.
2. Any employee of a non-U.S. Affiliate of Castle engaged in the export from a country other than the U.S. of goods, services or technology of U.S. origin or containing U.S.-origin material or component parts must determine and document whether a reexport license issued by the Department of Commerce or Department of State is required prior to shipment and, if so, ensure that the requisite reexport license has been obtained before reexport. Generally, products requiring an export license prior to shipment from the U.S. to a particular destination will require a license prior to reexport by a non-U.S. Affiliate to that destination, unless the U.S.-origin content is below a specified regulator threshold. Please contact the Trade Compliance Department for assistance.

Castle, its subsidiaries and its employees may incur significant civil and/or criminal penalties for violating U.S. sanctions programs, Antiboycott, corrupt practices, and export control laws and regulations. Therefore, all directors, officers, employees, agents, and other representatives of Castle and its worldwide subsidiaries shall comply with the procedures defined in this policy.

EMPLOYEE RESPONSIBILITIES

This Policy imposes on all employees specific responsibilities and obligations that will be enforced through standard disciplinary measures and properly reflected in employee evaluations.

All officers, employees and agents are responsible for understanding and complying with the Policy, as it relates to their jobs. Every employee has an obligation to:

- Be familiar with applicable aspects of the Policy and communicate them to subordinates;
- Ask questions if the Policy or action required to take in a particular situation is unclear;
- Properly manage and monitor business activities conducted through third-parties;
- Be alert to indications or evidence or possible wrongdoing; and
- Promptly report violations or suspected violations through appropriate channels.

The Company's managers have a particular responsibility to ensure that subordinates, including agents, receive proper training, and to monitor for compliance with the Policy.

REPORTING POSSIBLE VIOLATIONS

Any employee who has reason to believe that a violation of this Policy has occurred, or may occur, must promptly report this information to his or her supervisor, the next level of supervision or the General Counsel. Alternatively, information may be reported in confidence by calling the A. M. Castle Compliance Hotline (1-800-461-9330). Retaliation in any form against an employee who has, in good faith, reported a violation or possible violation of this Policy is strictly prohibited.

Employees who violate this Policy will be subject to disciplinary action, up to and including dismissal. Violations can also result in prosecution by law enforcement authorities and serious criminal and civil penalties.